

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-171510  
(P2002-171510A)

(43)公開日 平成14年6月14日(2002.6.14)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
H 0 4 N 7/173 5/44	6 1 0	H 0 4 N 7/173 5/44	6 1 0 Z 5 C 0 2 5 A 5 C 0 6 4 Z

審査請求 未請求 請求項の数9 O L (全 10 頁)

(21)出願番号 特願2000-367832(P2000-367832)

(22)出願日 平成12年12月1日(2000.12.1)

(71)出願人 000006079  
ミノルタ株式会社  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル  
(72)発明者 原 吉宏  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内  
(72)発明者 出山 弘幸  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内  
(74)代理人 100090446  
弁理士 中島 司朗

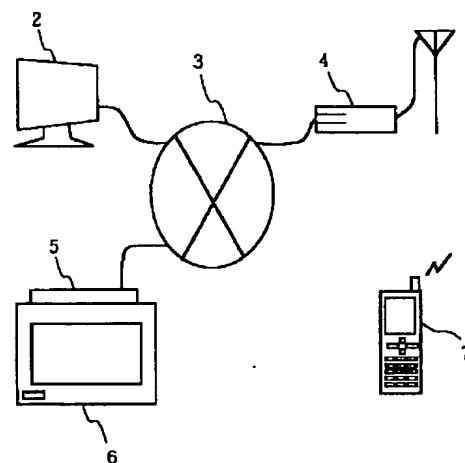
最終頁に続く

(54)【発明の名称】 画像サーバ装置、当該画像サーバ装置を用いた画像通信システム

(57)【要約】

【課題】 デジタル画像をサーバ装置に格納すると、必要な範囲に自動的にその旨を通知する画像通信システムを提供する。

【解決手段】 画像データを格納する複数の記憶領域を有する記憶装置を備えた画像サーバ装置4と端末2、5、7をネットワーク接続した画像通信システムにおいて、画像サーバ装置4は、画像データを格納する少なくとも1の記憶領域を有する記憶装置と、画像データの前記記憶装置への格納を要求する格納要求であって、当該画像データを格納する記憶領域を指定する領域指定を含む格納要求を提供端末から受け付ける格納要求受付手段と、領域指定により指定された記憶領域に画像データを書き込む書き込み手段と、画像データを格納した旨を通知する格納通知の宛先となる表示端末を、前記領域指定を用いて決定する宛先決定手段と、宛先決定手段により決定された宛先に、格納通知を送信する格納通知手段とを備える。



**【特許請求の範囲】**

【請求項 1】 ネットワークを介して接続される端末装置に対して、閲覧属性に応じて画像データの参照を許可する画像サーバ装置であって、  
閲覧属性を付与して画像データを記憶する記憶手段と、  
閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付手段と、  
画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定手段と、  
決定された宛先に前記記憶通知を送信する記憶通知手段とを備えることを特徴とする画像サーバ装置。

【請求項 2】 閲覧属性に対応する記憶領域を決定する記憶領域決定手段を備え、  
前記記憶手段は、決定された記憶領域に画像データを記憶することを特徴とする請求項 1 に記載の画像サーバ装置。

【請求項 3】 前記各記憶領域に対応付けて第 1 の認証情報を記憶する第 1 の認証情報記憶手段と、  
前記端末装置から画像データの参照を要求する第 1 の参照要求を受け付ける第 1 の参照要求受付手段と、  
前記決定された宛先以外の端末装置から前記第 1 の参照要求を受け付けた場合、要求された画像データを記憶する記憶領域に対応付けられた第 1 の認証情報と当該端末装置から受け付けた第 2 の認証情報とを照合して、画像データの参照を許可するかどうかを決定する参照許可手段とを備えることを特徴とする請求項 2 に記載の画像サーバ装置。

【請求項 4】 メッセージを含む前記記憶要求を受け付けるメッセージ付き記憶要求受付手段と、  
前記記憶要求に係る画像データに関連付けて前記メッセージを記憶するメッセージ記憶手段と、  
当該記憶要求に係る画像データの参照を端末装置から要求されると、当該記憶要求に含まれたメッセージを返信するメッセージ返信手段を備えることを特徴とする請求項 3 に記載の画像サーバ装置。

【請求項 5】 前記メッセージを返信された端末装置から返信メッセージを受け付ける返信メッセージ受付手段と、  
前記メッセージに関連付けて前記返信メッセージを記憶する返信メッセージ記憶手段と、  
受け付けた返信メッセージを、前記メッセージを含む記憶要求の要求元である端末装置に転送する返信メッセージ転送手段を備えることを特徴とする請求項 4 に記載の画像サーバ装置。

【請求項 6】 画像データを提供する画像提供端末、画像データを表示する画像表示端末、および請求項 1 に記載の画像サーバ装置をネットワーク接続した画像通信システムであって、

画像提供端末は、画像サーバ装置に記憶要求を送信する記憶要求手段を備え、  
画像表示端末は、画像サーバ装置から記憶通知を受信する通知受信手段と、  
記憶通知を受信した旨を表示する通知表示手段とを備えることを特徴とする画像通信システム。

【請求項 7】 前記画像サーバ装置は、記憶要求に係る画像データの指定と閲覧属性とを記憶する指定情報記憶手段と、  
記憶通知に係る画像データの参照を要求する第 2 の参照要求を表示端末から受け付ける第 2 の参照要求受付手段と、  
第 2 の参照要求を送信した表示端末に当該要求に係る画像データを返信する画像データ返信手段とを備え、  
前記表示端末は、第 2 の参照要求を送信する第 2 の参照要求手段と、  
第 2 の参照要求に対して返信された画像データを画像サーバ装置から受信する画像データ受信手段とを備えることを特徴とする請求項 6 に記載の画像通信システム。

【請求項 8】 端末装置に対して閲覧属性に応じて画像データの参照を許可する画像サーバ装置と、端末装置とをネットワーク接続した画像通信システムにおいて、  
閲覧属性を付与して画像データを記憶する記憶ステップと、  
閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付ステップと、  
画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定ステップと、  
決定された宛先に記憶通知を送信する記憶通知ステップとを前記画像サーバ装置に実行させることを特徴とする画像通信方法。

【請求項 9】 請求項 8 に記載の画像通信方法を画像サーバ装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】 本発明は画像データを格納するサーバ装置とネットワークを介して当該サーバ装置に画像データに格納したり、格納された画像データを参照したりする端末装置からなる画像通信システムに関し、特に画像データに対する端末装置からのアクセスをサーバ装置に管理させる画像通信システムに関する。

**【0002】**

【従来の技術】 近年、パソコンやデジタルカメラ等の普及によりデジタル画像が非常に身近なものとなってきている。デジタル画像はインターネット等のネットワークを介して容易に伝送することができるため、サーバ装置にデジタル画像を蓄えて、端末装置（パソコン、携帯電

話等)から参照させる画像通信システムが盛んに利用されている。例えば、ネットワークを介して投稿されたデジタル画像をホームページにて参照させるサービスが提供されており、このようなシステムでは不特定多数の利用者がデジタル画像を发表或、参照したりすることができる。

【0003】このようなサービスを利用してデジタル画像を参照する場合、新規なデジタル画像が投稿されたかどうかを予め知ることができないため、サーバ装置に空しく何度もアクセスして、新規なデジタル画像が投稿されていないことを確認する破目となることもしばしばである。これに対して、例えば特開2000-20371号公報に開示の情報ライブラリー・サーバー／クライアントシステムは、情報ライブラリー・サーバーに新規に登録された情報ファイルに添付された情報タイトルと、情報タイトルと通知先グループを対応付ける登録情報・通知情報ファイルと、各通知先グループ名に属する通知先を定義した通知先グループテーブルとを参照して、情報ファイルが新規に登録された旨を通知する通知先を決定することによって当該通知先に先の旨を通知するというものである。

【0004】このようにすれば、新規に情報ファイルが登録されたことが通知されるので、徒らに情報ライブラリー・サーバーにアクセスすることを回避できる。

【0005】

【発明が解決しようとする課題】近年、情報システムにおけるセキュリティの強化が強く求められており、情報ファイルについてもアクセス権を設定する必要がある。これに対して上記の従来技術は情報ファイルに対するアクセス権に関わらず前記通知を行うため、情報ファイルの新規登録を通知された者がアクセス権の制限により当該情報ファイルを参照できない場合がある。

【0006】この問題を解消するには前記通知先グループ・テーブルに通知先グループ毎の通知先を設定する際に情報ファイルに対するアクセス権を考慮する必要があるのだが、情報ファイルに対するアクセス権に設定が変更されるたびに通知先の設定を変更することは極めて煩瑣な作業であるし、そもそもアクセス権を考慮して通知先を設定すること自体が困難である。

【0007】本発明は、上記のような問題に鑑みてなされたものであって、デジタル画像をサーバ装置に格納すると、当該デジタル画像に関するアクセス権に応じて格納を通知する画像通信システムを提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、本発明に係る画像サーバ装置は、ネットワークを介して接続される端末装置に対して、閲覧属性に応じて画像データの参照を許可する画像サーバ装置であって、閲覧属性を付与して画像データを記憶する記憶手段と、閲

覧属性を指定して前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付手段と、画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定手段と、決定された宛先に前記記憶通知を送信する記憶通知手段とを備えることを特徴とする。このようにすれば、デジタル画像をサーバ装置に格納するだけで、当該デジタル画像に関するアクセス権に応じて当該デジタル画像の格納を通知させることができる。

【0009】また、閲覧属性に対応する記憶領域を決定する記憶領域決定手段を備え、前記記憶手段は、決定された記憶領域に画像データを記憶することを特徴とする。また、前記各記憶領域に対応付けて第1の認証情報を記憶する第1の認証情報記憶手段と、前記端末装置から画像データの参照を要求する第1の参照要求を受け付ける第1の参照要求受付手段と、前記決定された宛先以外の端末装置から前記第1の参照要求を受け付けた場合、要求された画像データを記憶する記憶領域に対応付けられた第1の認証情報と当該端末装置から受け付けた第2の認証情報とを照合して、画像データの参照を許可するかどうかを決定する参照許可手段とを備えることを特徴とする。

【0010】また、メッセージを含む前記記憶要求を受け付けるメッセージ付き記憶要求受付手段と、前記記憶要求に係る画像データに関連付けて前記メッセージを記憶するメッセージ記憶手段と、当該記憶要求に係る画像データの参照を端末装置から要求されると、当該記憶要求に含まれたメッセージを返信するメッセージ返信手段を備えることを特徴とする。このようにすれば、デジタル画像に併せて、当該デジタル画像に関するメッセージを伝達させることができる。

【0011】また、前記メッセージを返信された端末装置から返信メッセージを受け付ける返信メッセージ受付手段と、前記メッセージに関連付けて前記返信メッセージを記憶する返信メッセージ記憶手段と、受け付けた返信メッセージを、前記メッセージを含む記憶要求の要求元である端末装置に転送する返信メッセージ転送手段を備えることを特徴とする。このようにすれば、前記メッセージに対する応答のメッセージを返信することができるので、特定のデジタル画像をトピックスとしてユーザ間のコミュニケーションを図ることができる。

【0012】また、本発明に係る画像通信システムは、画像データを提供する画像提供端末、画像データを表示する画像表示端末、および請求項1に記載の画像サーバ装置をネットワーク接続した画像通信システムであって、画像提供端末は、画像サーバ装置に記憶要求を送信する記憶要求手段を備え、画像表示端末は、画像サーバ装置から記憶通知を受信する通知受信手段と、記憶通知を受信した旨を表示する通知表示手段とを備えることを特徴とする。

【0013】また、前記画像サーバ装置は、記憶要求に係る画像データの指定と閲覧属性とを記憶する指定情報記憶手段と、記憶通知に係る画像データの参照を要求する第2の参照要求を表示端末から受け付ける第2の参照要求受付手段と、第2の参照要求を送信した表示端末に当該要求に係る画像データを返信する画像データ返信手段とを備え、前記表示端末は、第2の参照要求を送信する第2の参照要求手段と、第2の参照要求に対して返信された画像データを画像サーバ装置から受信する画像データ受信手段とを備えることを特徴とする。

【0014】また、本発明に係る画像通信方法は、端末装置に対して閲覧属性に応じて画像データの参照を許可する画像サーバ装置と、端末装置とをネットワーク接続した画像通信システムにおいて、閲覧属性を付与して画像データを記憶する記憶ステップと、閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付ステップと、画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定ステップと、決定された宛先に記憶通知を送信する記憶通知ステップとを前記画像サーバ装置に実行させることを特徴とする。

【0015】また、本発明に係る記録媒体は、コンピュータ読み取り可能な記録媒体であって、前記画像通信方法を画像サーバ装置に実行させるプログラムが記録されている。

#### 【0016】

【発明の実施の形態】以下、本発明に係る画像通信システムの実施の形態を、図面を参照しながら説明する。

（実施の形態）図1は、本発明に係る画像通信システム1を示した図である。画像通信システム1は、一家庭内に敷設されたホームネットワーク3にホームサーバ4、パーソナルコンピュータ2、テレビ受像機6が接続されており、更にホームサーバ4は公衆回線を介して随時、携帯電話7に接続される。パーソナルコンピュータ2、ホームサーバ4、テレビ受像機6は互いにTCP/IP（Transmission Control Protocol/Internet Protocol）を用いてデジタル画像等のデータを交換する。

【0017】なお、テレビ受像機6にはセットトップボックス5が搭載されており、当該セットトップボックス5を介してホームネットワーク3に接続されている。セットトップボックス5は、外部インターフェースとしてアンテナ端子、ビデオ出力端子等を備え、また、チューナを内蔵している。前記アンテナ端子にはテレビアンテナが接続されている。前記ビデオ出力端子はテレビ受像装置のビデオ入力端子に接続されており、セットトップボックス5が前記チューナにて受信したテレビ映像をテレビ受像装置に表示させる。また、セットトップボックス5はシリアルポートを有しており、当該ポートにデジタルカメラ等を接続して、デジタル画像を電子ファイル

（例えば、MPEGファイル）の形式で、セットトップボックス5に内部記憶装置に格納させることができる。

【0018】図2は、前記セットトップボックス5に付属のリモートコントローラを示した図である。セットトップボックス5は不図示の赤外線ポートを有しており、リモートコントローラ10は赤外線ポート16を用いて、セットトップボックス5と通信する。リモートコントローラ10は、電源ボタン11、チャンネルボタン17等を備えており、電源ボタン11はセットトップボックス5の電源をオンオフさせるためのボタンである。チャンネルボタン17は、テレビ受像装置に表示させるチャンネルを選択するためのボタンであり、後述のようにテキスト入力にも用いる。テレビボタン18は、テレビ受像装置にテレビ番組を表示させるために用いるボタンである。カーソルキー12～15、およびボタン19～21の機能については後述する。

【0019】さて、画像通信システム1の利用者は、パーソナルコンピュータ2に格納されたデジタル画像を、次のようにしてホームサーバ4に格納させる。まず、パーソナルコンピュータ2においてブラウザを起動し、ホームサーバ4のWebページを表示させる。図3は、ホームサーバ4のエントリ画面に相当するWebページである。エントリ画面30には、タイトル文字31、ホームサーバ4に格納されたデジタル画像を参照するための参照ボタン32、およびホームサーバ4にデジタル画像を格納するための登録ボタン33が表示される。

【0020】利用者が登録ボタン33をクリックすると、格納すべきデジタル画像の電子ファイル名を入力させるウィンドウ、すなわち登録画面が表示される。図4は、デジタル画像をホームサーバ4の記憶装置に格納させるための登録画面である。登録画面40には、デジタル画像を格納するホームサーバ内のフォルダを指定させるテキストボックス41、ホームサーバ4の記憶装置に格納させるデジタル画像を表示させる画像表示エリア42、デジタル画像とともにホームサーバに送付するメッセージを入力させるテキストボックス43、および登録ボタン44が配されている。

【0021】利用者は、テキストボックス41、43へはキーボードを用いてテキストを入力し、デジタル画像の指定についてはファイルマネージャ等からデジタル画像を格納した電子ファイルを画像表示エリア42にドラッグして表示させることにより行う。登録ボタン44は、テキストボックス41、43への入力完了後にクリックされるボタンであって、当該登録ボタン44がクリックされると、テキストボックス41、43に入力された内容と画像表示エリア42に表示されたデジタル画像データが、ホームサーバ4に送付される。

【0022】また、画像通信システム1の利用者は、前記セットトップボックス5の内部記憶装置に格納されたデジタル画像をホームサーバ4に格納させる場合には、

次のようにする。リモートコントローラ10の画像ボタン19が押下されると、テレビ受像機6にホームサーバ4のエントリ画面30が表示される。ここで、カーソルキー12～15を操作して登録ボタン33を選択し、リモートコントローラ10の完了ボタン21を押下すると、今度はテレビ受像機6に登録画面40が表示される。カーソルキー12～15を操作してテキストボックス41を選択し、リモートコントローラ10の表示ボタン19を押下すると、フォルダ名を列挙したプルダウンメニューが表示される。利用者は、更にカーソルキー12～15を操作して、プルダウンメニューに表示されたフォルダのうち、デジタル画像を格納したいフォルダを反転表示させたのち、リモートコントローラ10の完了ボタン21を押下すると、反転表示させたフォルダ名がテキストボックス41に入力される。

【0023】デジタル画像の指定については、まず画像表示エリア42を選択した後、表示ボタン20を押下すると、画像表示エリア42にデジタル画像が表示される。この時、カーソルキー12～15を操作すると、セットトップボックス5の内部記憶装置に格納されたデジタル画像が順に画像表示エリア42に表示されるので、ホームサーバ4に格納したいデジタル画像を表示させた後、完了ボタン21を押下すると、当該デジタル画像が選択される。

【0024】メッセージについては、テキストボックス43を選択した後、チャンネルボタン17を用いて、テキストボックス43に入力する。これらの入力完了したら、更にカーソルキー12～15を操作して登録ボタン44を選択し、完了ボタン21を押下すると、テキストボックス41、43に入力された内容と画像表示エリア42に表示されたデジタル画像が、ホームサーバ4に送付される。すなわち、ホームサーバ4に対する格納要求として、デジタル画像を格納する領域を指定するフォルダ名、デジタル画像、およびメッセージが送信される。

【0025】次に、ホームサーバ4について説明する。ホームページ4は、大容量の内部記憶装置を備えており、当該内部記憶装置にはデジタル画像を格納する複数のフォルダと、各端末装置からの格納されたデジタル画像に対するアクセスをフォルダ毎に管理するアクセス管理テーブルを備えている。図5は、アクセス管理テーブルを例示した図である。図5のアクセス管理テーブルには、利用者の家族構成（父、母、長男、次男、長女）に合わせた、共用フォルダ、パパ用フォルダ、ママ用フォルダ、太郎用フォルダ、次郎用フォルダ、花子用フォルダの計6つのフォルダに対する端末装置（パーソナルコンピュータ2、テレビ受像機6、携帯電話7）からのアクセスの可否に関する情報が設定されている。

【0026】アクセス管理テーブルにおいて、アクセス可否についての設定「A」は、端末装置からフォルダ

に対して当該フォルダに格納されたデジタル画像を参照する要求があると、ホームサーバ4は無条件に許可すべきことを意味する。設定「B」は、端末装置からフォルダに対して当該フォルダに格納されたデジタル画像の参照要求があると、ホームサーバ4は端末装置に対してパスワードを要求し、正しいパスワードが入力された時のみアクセスを許可すべきことを意味する。設定「C」は、端末装置からフォルダに対してデジタル画像の参照要求があると、ホームサーバ4は無条件に拒絶すべきことを意味する。なお、端末装置からフォルダに対してデジタル画像を格納する要求がきた場合には、ホームサーバ4はアクセス管理テーブルを参照せず、無条件にこれを許可する。

【0027】図5のアクセス管理テーブルにおいて、パーソナルコンピュータ2またはテレビ受像機6から共用フォルダに格納されたデジタル画像を参照する場合には無条件に許可されるように、またそれらの端末装置から共用フォルダ以外のフォルダに格納されたデジタル画像を参照する場合には、各フォルダに割り当てられたパスワードを入力するような設定となっている。また、携帯電話7は屋外に持ち出す都合上、セキュリティ確保のために、共用フォルダに格納されたデジタル画像を参照する場合のみパスワードの入力を条件としてアクセスを許可し、共用フォルダ以外のフォルダに格納されたデジタル画像については無条件にアクセスを禁止する設定としている。

【0028】さて、前述のように各端末装置からホームサーバ4に対してデジタル画像の格納要求が発せられると、ホームサーバ4は当該要求に従ってデジタル画像とメッセージを所定のフォルダに格納する。図6は、端末装置からデジタル画像の格納要求を受信したホームサーバ4の動作を示したフローチャートである。ホームサーバ4は、デジタル画像を指定されたフォルダに格納すると（ステップS1）、アクセス管理テーブルの当該フォルダに対応する列を参照して、各端末装置について順に設定を参照する。すなわち、アクセス管理テーブル中で設定を未参照の端末装置を検索して（ステップS2）、そのような端末装置を発見したら（ステップS3でYES）、設定を参照する（ステップS4）。この設定が上記「A」、「B」、「C」の各設定のうちの「A」であれば（ステップS5でYES）、当該端末装置にフォルダに新規なデジタル画像を格納した旨の通知、すなわち格納通知を送付する（ステップS6）。ステップS4で参照した設定が「B」または「C」ならば（ステップS5でNO）、ステップS2に進んで再び設定を未参照の端末装置を検索する。そうして、未参照の端末装置が見つからなければ（ステップS3でNO）、処理を終了する。なお、ホームサーバ4は、デジタル画像を記憶装置に格納する際に、当該デジタル画像の格納を要求した端末装置の識別情報を登録元情報として併せて格納する。

【0029】次に、端末装置からホームサーバ4の記憶装置に格納されたデジタル画像を参照する際の処理について、セットトップボックス5、パーソナルコンピュータ2、携帯電話7の順に説明する。ホームサーバ4の記憶装置に格納されたデジタル画像をテレビ受像機6に表示させるために、利用者はセットトップボックス5を次のように操作する。図7は、デジタル画像をテレビ受像機6に表示させるための典型的な操作手順を示したフローチャートである。利用者は、先ずリモートコントローラ10を操作してセットトップボックス5の電源を投入する（ステップS10）。次に、画像ボタン19を押下してテレビ受像機6にエントリ画面30を表示させ（ステップS11）、当該エントリ画面30中の参照ボタン32をクリックする（ステップS12）。なお、参照ボタン32のクリックの仕方については、上述した登録ボタン33のクリックの仕方と同様である。利用者が登録ボタン33をクリックすると、テレビ受像機6に参照画面が表示される。

【0030】図8は、デジタル画像の電子ファイル名を入力させるための参照画面である。参照画面50には、表示させたいデジタル画像を格納したホームサーバ内のフォルダを指定させるテキストボックス51、デジタル画像を表示させる画像表示エリア52、デジタル画像とともにホームサーバに格納されているメッセージを表示させるテキストボックス53、前記メッセージに対する返信メッセージを入力させるテキストボックス54、および返信ボタン55が配されている。

【0031】利用者は、リモートコントローラ10のカーソルキー12～15を操作してテキストボックス51を選択し、リモートコントローラ10の表示ボタン19を押下すると、フォルダ名を列挙したプルダウンメニューが表示される。利用者は、更にカーソルキー12～15を操作して、プルダウンメニューに表示されたフォルダのうち、所望のフォルダを反転表示させたのち、リモートコントローラ10の完了ボタン21を押下すると、反転表示させたフォルダ名がテキストボックス51に表示される（ステップS13）。

【0032】完了ボタン21が押下されると、端末装置名（セットトップボックス5）とフォルダ名を伴って、その旨の通知がセットトップボックス5からホームサーバ4になされる。するとホームサーバ4は、通知された端末装置名とフォルダ名に対応する前記アクセス管理テーブルの設定を参照して、当該設定が「B」ならば、セットトップボックス5を介してテレビ受像機6にパスワードを要求するウィンドウを表示させる。利用者は、このようにしてパスワードを要求されると（ステップS14でYES）、当該ウィンドウにパスワードを入力する（ステップS15）。

【0033】すると、当該パスワードがホームサーバ4に転送される。ホームサーバ4は、受信したパスワード

と記憶装置に保存されているパスワードとを照会して一致したら、アクセスを許可する旨のメッセージを表示するウィンドウをテレビ受像機6に表示させる。受信したパスワードが正しくなければ、アクセスを拒絶する旨のメッセージを表示するウィンドウをテレビ受像機6に表示させる。

【0034】利用者は、パスワードを要求されなければ（ステップS14でNO）、またはホームサーバ4によりアクセスを許可されたら、参照画面50上で画像表示エリア52を選択した後、表示ボタン20を押下すると、画像表示エリア52にデジタル画像が表示される。この時、カーソルキー12～15を操作すると、セットトップボックス5の内部記憶装置に格納されたデジタル画像が順に画像表示エリア52に表示される（ステップS16）。

【0035】このとき同時に、画像表示エリア52に表示されたデジタル画像がホームサーバ4に格納された時に併せて格納されたメッセージがテキストボックス53に表示される。利用者が当該メッセージに対して応答したい場合には（ステップS17でYES）、登録画面でメッセージを入力したのと同様の手順で、テキストボックス54に返信メッセージを入力した後（ステップS18）、返信ボタン55をクリックすると（ステップS19）、テキストボックス54に入力した返信メッセージがホームサーバ4に送付される。なお、返信メッセージにはテキストボックス51に表示されたフォルダ名と画像表示エリアに表示されたデジタル画像の識別子が自動的に添付されている。また、デジタル画像の識別子は当該デジタル画像をホームサーバ4が端末装置に送付する時に自動的に添付される。

【0036】本発明に係る画像通信システム1を用いて、ホームサーバ4の記憶装置に格納されたデジタル画像をテレビ受像機6に表示させる場合、上記のほかに次のような操作手順も許される。セットトップボックス5はホームサーバ4から上述の格納通知を受信すると、テレビ受像機6に格納通知を受信した旨のメッセージをテロップ（TELOP: Television Opaque Projector）表示させる。このテロップ表示は所定時間（10秒間）だけ継続し、その後、自動的にテロップ表示を終了する。当該テロップが表示されている期間中に利用者がリモートコントローラ10の画像ボタン19を押下すると、その旨がセットトップボックス5からホームサーバ4に直ちに通知され、通知を受けたホームサーバ4はテレビ受像機6に参照画面50を表示させる。この時、参照画面50のテキストボックス51、53には自動的にフォルダ名とメッセージが、画像表示エリア52には自動的にデジタル画像が表示される。このようにすれば、格納通知を受信した際に、簡単な手順で新規に追加されたデジタル画像を参照することができる。

【0037】なお、ホームサーバ4は、端末装置に格納

通知を送信する際に、当該格納通知に係る諸情報（デジタル画像、メッセージ、格納を要求した端末装置等）を端末装置毎に格納通知テーブルに格納しており、上記のように格納通知に係るデジタル画像の参照を端末装置から要求されると、当該格納通知テーブルを参照して最後に送信した格納通知に係るデジタル画像の参照を要求した端末装置に返信する。また、このとき格納通知テーブルにメッセージが格納されていたら、当該メッセージも併せて端末装置に返信する。

【0038】テレビ受像機6に代えてパーソナルコンピュータ2を用いて、ホームサーバ4に格納されたデジタル画像を参照する手順についても概ね同様であるが、テレビ受像機6の場合におけるテロップ表示については、特に次に述べるようにする。すなわち、ホームサーバ4からの格納通知を受信して、格納通知を受信した旨をパーソナルコンピュータ2の表示画面上にポップアップ表示させるプログラムをパーソナルコンピュータ2に常駐させて、以下の処理を遂行させる。

【0039】図9は、当該常駐プログラムがパーソナルコンピュータ2の表示画面上にポップアップ表示させるポップアップウィンドウを示した図である。パーソナルコンピュータ2の常駐プログラムはホームサーバ4から格納通知を受信すると図9のような格納通知画面を表示したポップアップウィンドウを表示する。格納通知画面にはホームサーバ4に新規なデジタル画像が登録された旨のメッセージ61と、当該デジタル画像を参照させるための参照ボタン62が表示されている。

【0040】パーソナルコンピュータ2の利用者が前記参照ボタン62をクリックすると、その旨がパーソナルコンピュータ2からホームサーバ4に直ちに通知され、通知を受けたホームサーバ4はパーソナルコンピュータ2に参照画面50を表示させる。この時、参照画面50のテキストボックス51、53には自動的にフォルダ名とメッセージが、画像表示エリア52には自動的にデジタル画像が表示される。このようにすればテレビ受像機の場合と同様にして、格納通知を受信した際に、簡単な手順で新規に追加されたデジタル画像を参照することができる。

【0041】さて、端末装置（パーソナルコンピュータ2またはセットトップボックス5）から返信メッセージを受信したホームサーバ4は、返信メッセージに添付されたフォルダ名とデジタル画像の識別子を用いて記憶装置に格納されたデジタル画像を特定し、特定したデジタル画像に付随して記憶装置に格納されている当該デジタル画像の登録元情報を参照し、前記返信メッセージを当該デジタル画像の登録元に転送する。

【0042】セットトップボックス5は、ホームサーバ4から返信メッセージを受信すると、その旨を示すテロップをテレビ受像機に表示させる。このテロップ表示は、格納通知を受信した旨のテロップと同様に、所定時

間（10秒間）だけ継続した後、自動的に終了する。当該テロップが表示されている期間中に利用者がリモートコントローラ10の画像ボタン19を押下すると、その旨がセットトップボックス5からホームサーバ4に直ちに通知され、通知を受けたホームサーバ4はテレビ受像機6に返信メッセージ参照画面を表示させる。図10は、返信メッセージ参照画面を示した図である。返信メッセージ参照画面70の画像表示エリア71にはデジタル画像が、テキストボックス72、73には返信メッセージと当該返信メッセージの発信元端末装置の名称がそれぞれ表示される。

【0043】パーソナルコンピュータ2がホームサーバ4から返信メッセージを受信する場合については、前記格納通知を受信する場合と同様に、パーソナルコンピュータ2に常駐する常駐プログラムが返信メッセージを受信して、図10と同様の返信メッセージ参照画面を表示したポップアップウィンドウを表示する。以上のようにすれば、ホームサーバ4に新規なデジタル画像を登録した際に、当該デジタル画像に関連する端末装置にのみ自動的にその旨が通知されるので、新規デジタル画像がホームサーバ4に格納されたかどうかをチェックするために端末装置から頻繁に参照しにゆくという無駄な手間を省くことができるのみならず、各利用者による端末装置の占有時間を低減させて端末装置の利用効率を高めることができるので、ネットワークの負荷や電力消費等を低減させることができる。

（変形例）以上、本発明を実施の形態に基づいて説明してきたが、本発明は、上述の実施の形態に限定されないのは勿論であり、以下のような変形例を実施することができる。

【0044】上記実施の形態においては、アクセス管理テーブルでの設定が「B」の場合、必ずパスワードを問い合わせるとしたが、パーソナルコンピュータ2のようにログイン時にパスワード等により認証を行う端末装置については、次のようにしてパスワードの問い合わせをスキップするとしてもよい。図11は、本変形例に係る画像通信システムのホームサーバに格納されたアクセス管理テーブルを示した図である。当該アクセス管理テーブルが上記実施の形態に係るアクセス管理テーブルと異なる点は、パーソナルコンピュータ2からのアクセスについての設定がすべて「A」となっている点である。パーソナルコンピュータはログイン時にパスワードを要求するので、このように設定してパスワードの入力回数を削減してもセキュリティを保つことができる。

【0045】また、図12は、このような機能を有するアクセス管理テーブルの別の変形例である。図12のアクセス管理テーブルは、端末装置毎にタイプ設定欄を設けて、パスワードの要、不要を設定させる。前記のようにログイン時等に認証を行う端末装置については当該タイプ設定欄に「フリー」と設定して、ホームサーバ4か

らのパスワードの問い合わせが不要である旨を表示し、タイプ設定欄に「チェック」と設定されている端末装置にのみホームサーバ4からパスワードの問い合わせを行わせる。

【0046】このようにすれば、パスワード等、認証情報を入力する回数を低減することができるので操作性をより高めることができる。なお、本発明は、上記に示す方法であるとしてもよいし、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよい。また、当該コンピュータプログラムをコンピュータ読み取り可能な記録媒体（フロッピー（登録商標）ディスク、ハードディスク、CD-ROM等）に記録したものとよい。

【0047】

【発明の効果】以上説明したように、本発明によれば、サーバ装置に新規デジタル画像を格納させる際に、その旨を自動的に所定の端末装置に通知させるので、新規画像が登録されていないことを確認するだけに終わるような無駄なアクセスを無くすることができる。したがって、サーバ装置に無駄にアクセスして落胆するような事態を回避できると共に、無駄なアクセスに伴って生じる電力やネットワーク資源の消費を低減することができる。

【0048】また、上記の通知を受ける端末装置を設定により予め指定できるので、そのような通知を必要としない端末装置に対して通知がなされることがない。したがって、通知の乱発によって通信等のログが急速に増大するような事態を回避できるので、当該ログの格納に消費されるサーバ装置や端末装置の固定記憶装置等の記憶容量を節約することができる。

【0049】更に、上記通知がなされた折には、デジタル画像の参照要求に対して自動的に当該通知に係るデジタル画像を端末装置に表示させるので、新規に格納されたデジタル画像を探し回る手間を省き、速やかに表示させることができる。したがって、そのような探し回りに伴う煩わしさを去り、画像通信システムの利用効率を向上させることができる。

【図面の簡単な説明】

【図1】本発明に係る画像通信システム1を示した図である。

【図2】セットトップボックス5に付属のリモートコン

トローラを示した図である。

【図3】ホームサーバ4のエントリ画面に相当するWebページである。

【図4】デジタル画像をホームサーバ4の記憶装置に格納させるための登録画面である。

【図5】アクセス管理テーブルを例示した図である。

【図6】端末装置からデジタル画像の格納要求を受信したホームサーバ4の動作を示したフローチャートである。

【図7】デジタル画像をテレビ受像機6に表示させるための典型的な操作手順を示したフローチャートである。

【図8】デジタル画像の電子ファイル名を入力させるための参照画面である。

【図9】常駐プログラムがパーソナルコンピュータ2の表示画面上にポップアップ表示させるポップアップウィンドウを示した図である。

【図10】返信メッセージ参照画面を示した図である。

【図11】変形例に係る画像通信システムのホームサーバ4に格納されたアクセス管理テーブルを示した図である。

【図12】変形例に係る画像通信システムのホームサーバ4に格納されたアクセス管理テーブルを示した図である。

【符号の説明】

- 1 画像通信システム
- 2 パーソナルコンピュータ
- 3 ホームネットワーク
- 4 ホームサーバ
- 5 セットトップボックス
- 6 テレビ受像機
- 7 携帯電話
- 10 リモートコントローラ
- 11 電源ボタン
- 12～15 カーソルキー
- 16 赤外線ポート
- 17 チャンネルボタン
- 18 テレビボタン
- 19 画像ボタン
- 20 表示ボタン
- 21 完了ボタン

【図5】

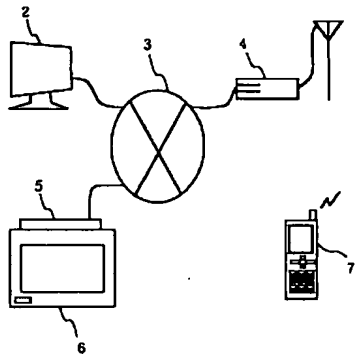
端末装置	フォルダ					
	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	A	B	B	B	B	B
テレビ受像機	A	B	B	B	B	B
携帯電話	B	C	C	C	C	C

【図11】

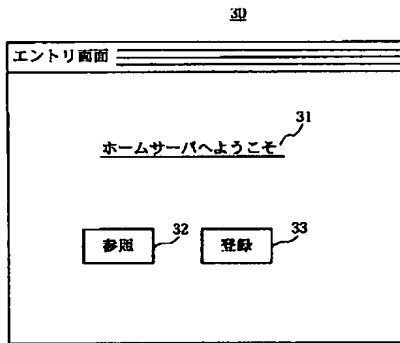
端末装置	フォルダ					
	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	A	A	A	A	A	A
テレビ受像機	A	B	B	B	B	B
携帯電話	B	C	C	C	C	C



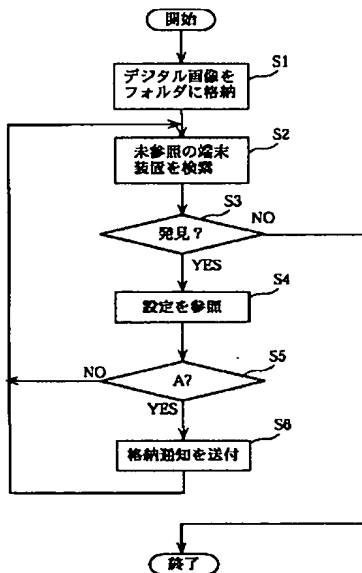
【図1】



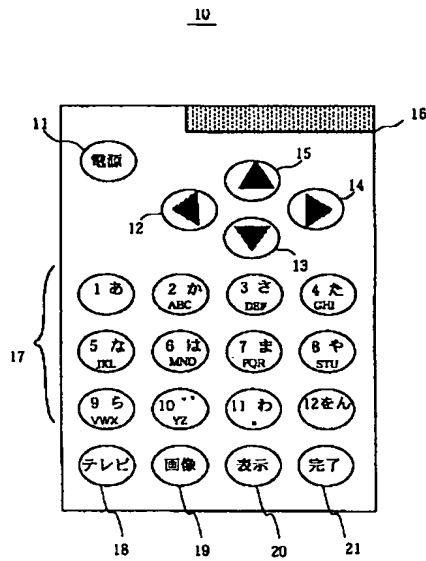
【図3】



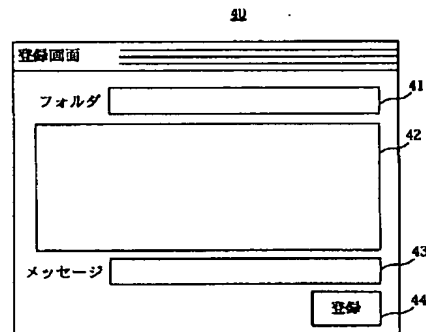
【図6】



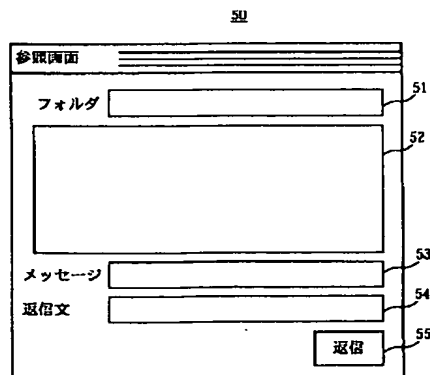
【図2】



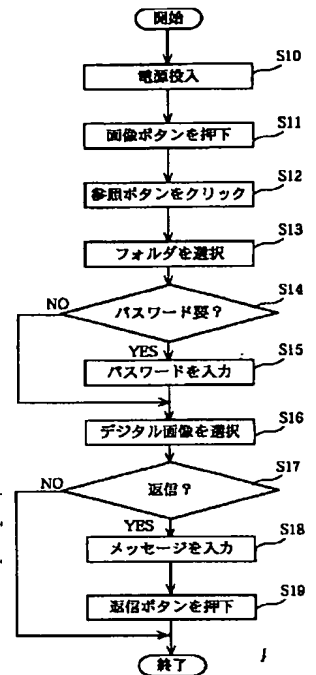
【図4】



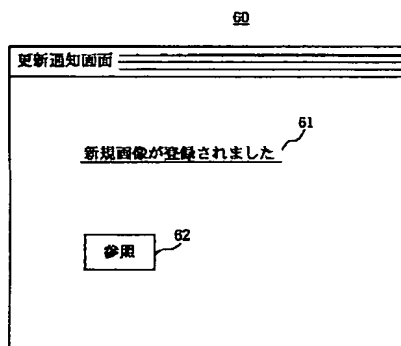
【図8】



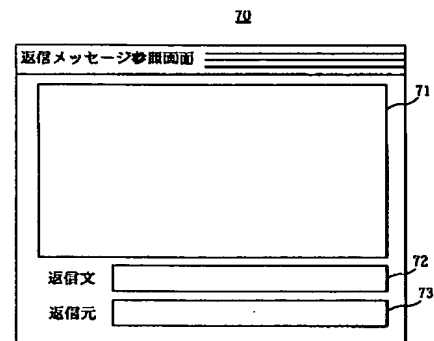
【図7】



【図9】



【図10】



【図12】

端末装置		フォルダ					
名称	タイプ	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	フリー	A	B	B	B	B	B
テレビ受像機	チェック	A	B	B	B	B	B
携帯電話	チェック	B	C	C	C	C	C

フロントページの続き

(72)発明者 藤井 巖  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内

(72)発明者 藤野 勤  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内

(72)発明者 高野 万滋  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内

(72)発明者 遠山 大雪  
大阪府大阪市中央区安土町二丁目3番13号  
大阪国際ビル ミノルタ株式会社内

Fターム(参考) 5C025 BA27 CA02 CA09 CB10 DA05  
5C064 BA01 BB10 BC18 BC23 BC25  
BD02 BD08

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-171510

(43)Date of publication of application : 14.06.2002

---

(51)Int.Cl. H04N 7/173

H04N 5/44

---

(21)Application number : 2000-367832 (71)Applicant : MINOLTA CO LTD

(22)Date of filing : 01.12.2000 (72)Inventor : HARA YOSHIHIRO

DEYAMA HIROYUKI

FUJII IWAO

FUJINO TSUTOMU

TAKANO KAZUSHIGE

TOOYAMA DAISETSU

---

(54) IMAGE SERVER UNIT AND IMAGE COMMUNICATION SYSTEM  
EMPLOYING THE IMAGE SERVER UNIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image communication system that automatically informs terminals within a required range about the storage of the digital image when a digital image is stored in a server unit.

SOLUTION: In the image communication system where the image server 4 provided with a storage device having storage areas to store image data and terminals 2, 5, 7 are interconnected through a network, the image server 4 is provided with the storage device that has at least one storage area to store image data, a storage request reception means that receives a storage request to request storage of image data to the storage device and including area designation to designate the storage area storing the image data from a data

providing terminal, a write means that writes the image data to a storage area designated by the area designation, a destination decision means that decides a display terminal acting like a destination of a storage notice, which the destination decision means informs of a fact of storing the image data, by using the area designation, and a storage notice means that transmits the storage notice to the destination decided by the destination decision means.

---

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

**\* NOTICES \***

**JPO and INPIT are not responsible for any  
damages caused by the use of this translation.**

1.This document has been translated by computer. So the translation may not  
reflect

the original precisely.

2.\*\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

**CLAIMS**

---

**[Claim(s)]**

**[Claim 1] It is a network connection system equipped with the network  
connection equipment for connecting to an external network the internal network  
which has two or more computers, and this internal network. An end is  
connected to said internal network and, as for said network connection**

equipment, the other end is connected to said external network. The switching means which changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, and when predetermined conditions are satisfied The network connection system characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[Claim 2] The network connection system according to claim 1 characterized by having further the fire wall which checks access to said internal network from said external network, and restricts access to an internal network between said internal networks and said external networks when this access is unlawful access.

[Claim 3] Said internal network and said external network It connects through the fire wall including an alarm generating means to generate an alarm when there is unlawful access to said internal network from said external network. It is the network connection system according to claim 1 characterized by realizing said network connection equipment as a function in said fire wall, and said control means making said switching means a substantial cutting condition when said alarm generating means generates an alarm.

[Claim 4] It is network connection equipment for connecting to an external

network the internal network which has two or more computers. The switching means which an end is connected to said internal network, and the other end is connected to said external network, and changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, Network connection equipment characterized by having the control means which changes whether said switching means is made into a substantial connection condition when predetermined conditions are satisfied, or it considers as a substantial cutting condition.

[Claim 5] It is network connection equipment according to claim 4 characterized by realizing said switching means and said control means as a function of a fire wall including an alarm generating means to generate an alarm when there is unlawful access to said internal network from said external network, respectively, and said control means making said switching means a substantial cutting condition when said alarm generating means generates an alarm.

[Claim 6] Said control means is network connection equipment according to claim 4 or 5 characterized by changing whether said switching means is made into a substantial connection condition according to generating of this predetermined event by supervising generating of the predetermined event in said internal network, or it considers as a substantial cutting condition.

[Claim 7] said control means -- a time check -- network connection equipment



given in claim 4 characterized by changing whether said switching means is made into a substantial connection condition when the time amount clocked by the means turns into predetermined time amount, or it considers as a substantial cutting condition thru/or any 1 term of 6.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the network connection system and equipment which connect internal networks, such as LAN (Local Area Network), and external networks, such as WAN (Wide Area Network).

[0002]

[Description of the Prior Art] Although it is increasingly used in a certain form,

carrying out network connection of the computer of recent years many, it has been a big technical problem how unlawful access to each computer is prevented. Especially in the network system to which internal networks, such as LAN, and external networks, such as WAN including the Internet, are connected, generally, the fire wall was prepared between the internal network and the external network, and each computer has prevented being unjustly accessed from an external network by the authentication and filtering by the fire wall.

[0003] However, each computer connected to the internal network also by the network connection system through a fire wall will always be fundamentally connected also with the external network. For this reason, it was impossible to have intercepted unlawful access from an external network completely. Then, in JP,2000-10887,A, the network interface module with a security switch is proposed as a technique for preventing unlawful access from the outside in each computer.

[0004] Drawing 4 is the block diagram showing the network interface module with a security switch of a publication in JP,2000-10887,A. The network interface module 101 is formed by 1 to 1 corresponding to a computer 105, and consists of a network interface 102 and a power-source interface 103 including the security switch 104 so that it may illustrate.

[0005] The power of the network interface module 101 is supplied from the

power source 107 in a computer 105. If CPU106 suspends supply of the power from a power source 107, the security switch 104 will turn off and a network interface 102 will serve as impossible of operation. It becomes impossible to access a computer 105 from an outside network by this, and unlawful access to a computer 105 can be prevented now.

[0006]

[Problem(s) to be Solved by the Invention] However, with the technique of a publication, the network interface module 101 must be formed in JP,2000-10887,A corresponding to each computer 105. However, by the system to which the internal network and the external network were connected, unlawful access to the computer 105 from an internal network can seldom be considered. It is useless from a tooth space and the field of cost to make a redundant configuration each of a computer 105 to such unlawful access that is hardly considered.

[0007] Moreover, if it is in the calculating machine further connected with the internal network in the external network, although an exchange of the data in an internal network is performed frequently, there are usually few exchanges of data with an external network overwhelmingly to this. For this reason, if the network interface module 101 is formed to each of a calculating machine 105 like JP,2000-10887,A and it can be made to carry out access refusal of each of a

calculating machine 105, trouble may arise in an exchange of the data only in an internal network.

[0008] This invention aims at offering the network access system which can exchange the data in an internal network efficiently while it prevents unjust access from an external network to the computer connected to the internal network.

[0009]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the network connection system concerning the 1st viewpoint of this invention It is a network connection system equipped with the network connection equipment for connecting to an external network the internal network which has two or more computers, and this internal network. An end is connected to said internal network and, as for said network connection equipment, the other end is connected to said external network. The switching means which changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, and when predetermined conditions are satisfied It is characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[0010] In the above-mentioned network connection system, when a control

means makes a switching means a substantial cutting condition, access to an internal network from an external network serves as impossible. This becomes possible to intercept unlawful access to an internal network from an external network. Here, even when the switching means is in the substantial cutting condition, the calculating machines in an internal network have kept the connection condition mutual, and trouble does not produce them in an exchange of the data in an internal network.

[0011] Between said internal networks and said external networks, the above-mentioned network connection system checks access to said internal network from said external network, and when this access is unlawful access, it shall be further equipped with the fire wall which restricts access to an internal network.

[0012] In the above-mentioned network connection system, said internal network and said external network may be connected through a fire wall including an alarm generating means to generate an alarm, when there is unlawful access to said internal network from said external network. In this case, said network connection equipment should be realized as a function in said fire wall, and said control means can make said switching means a substantial cutting condition, when said alarm generating means generates an alarm.

[0013] As it \*\*\*\*\* (ed), by using a fire wall together in addition to a switching

means, unlawful access to an internal network from an external network can be prevented more firmly, and it becomes possible to build a system with still higher security.

[0014] In order to attain the above-mentioned purpose, the network connection equipment concerning the 2nd viewpoint of this invention It is network connection equipment for connecting to an external network the internal network which has two or more computers. The switching means which an end is connected to said internal network, and the other end is connected to said external network, and changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, When predetermined conditions are satisfied, it is characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[0015] In the above-mentioned network connection equipment, said switching means and said control means may be realized as a function of a fire wall including an alarm generating means to generate an alarm, when there is unlawful access to said internal network from said external network, respectively. In this case, said control means can make said switching means a substantial cutting condition, when said alarm generating means generates an alarm.

[0016] In the above-mentioned network connection equipment, said control

means shall supervise generating of the predetermined event in said internal network, and shall change whether said switching means is made into a substantial connection condition according to generating of this predetermined event, or it considers as a substantial cutting condition again.

[0017] the above-mentioned network connection equipment -- setting -- said control means -- further -- a time check -- when the time amount clocked by the means turns into predetermined time amount, it shall change whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition

[0018]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to an accompanying drawing.

[0019] Drawing 1 is the block diagram showing the network connection structure of a system concerning the gestalt of this operation. In this network connection system, two or more computers 11 are connected to LAN1 as an internal network so that it may illustrate. LAN1 is connected to the circuit switch section 21 and a control section 22. The circuit switch section 21 and a control section 22 are contained in the internal network in large semantics. The other end of the circuit switch section 21 is connected to WAN3 as an external network. In addition, if it states concretely, LAN1 can be made into intranet and WAN3 can

be made into the Internet.

[0020] The circuit switch section 21 changes whether between LAN1 and WAN3 is made into a connection condition, or it considers as a cutting condition based on the control signal sent from the control section 22. A control section 22 generates and outputs the control signal which changes the condition of the circuit switch section 21 based on the control signal acquired from LAN1.

[0021] A control section 22 is realizable with the line board linked to LAN1, the personal computer which controls the circuit switch section 21. In this case, the circuit switch section 21 may be a cable switch which carries out ON/OFF of LAN1 and WAN3 physically with a serial signal. Moreover, the hardware of dedication may realize the circuit switch section 21 and a control section 22. In this case, the interface linked to LAN1 and the interface connected to WAN3 should just be offered.

[0022] Hereafter, the actuation in this network connection system is explained. Here, in the usual condition, the circuit switch section 21 shall be in a cutting condition.

[0023] Either of the events 11 which should connect LAN1 with WAN3, for example, a calculating machine, accesses the computer apparatus on WAN3, and when the event which is going to acquire data occurs, the calculating machine 11 concerned notifies the purport which is going to access WAN3 to a



control section 22. A control section 22 changes a control signal to the circuit switch section 21, and makes delivery and the circuit switch section 21 changed to a connection condition based on this notice.

[0024] After the circuit switch section 21 is in a connection condition, the calculating machine 11 concerned accesses the computer apparatus on WAN3, and acquires data from there. After acquisition of data is completed, the computer 11 concerned notifies the purport which ended access to WAN3 to a control section 22. A control section 22 changes a control signal to the circuit switch section 21, and makes delivery and the circuit switch section 21 changed to a cutting condition based on this notice.

[0025] On the other hand, when the computer apparatus on WAN3 tends to access either of the calculating machines 11 in LAN1, since the circuit switch section 21 is in the cutting condition, a calculating machine 11 cannot usually be accessed in fact. Also in this condition, since calculating-machine 11 comrades in LAN1 are in the connection condition, they can exchange data of each other freely.

[0026] As explained above, if the control section 22 makes the circuit switch section 21 the cutting condition, in the network connection system concerning the gestalt of this operation, the computer 11 in LAN1 cannot be accessed from WAN3. For this reason, since what is necessary is just to make the circuit switch

section 21 into the cutting condition altogether when the calculating machine 11 in LAN1 does not need to exchange WAN3 and data as an external network, it can protect being unjustly accessed by the calculating machine 11 in LAN1 from WAN3.

[0027] Moreover, even when the circuit switch section 21 is in a cutting condition, computer 11 comrades in LAN1 can always be maintaining the connection condition. For this reason, trouble does not arise in an exchange of the data of calculating-machine 11 comrades in LAN1, and processing in LAN1 can be performed efficiently.

[0028] This invention is not restricted to the gestalt of the above-mentioned operation, but various deformation and application are possible for it. Hereafter, the strange gestalt of the gestalt of the above-mentioned operation applicable to this invention is explained.

[0029] With the gestalt of the above-mentioned operation, the control section 22 had changed the circuit switch section 21 to the connection condition or the cutting condition based on the event generated in LAN1 which is an internal network. On the other hand, it is possible to change the circuit switch section 21 also according to the event generated in WAN3 which is an external network. But although the event generated in WAN3 is told to a control section 22 only when the circuit switch section 21 is in a connection condition, a control section

22 can change the circuit switch section 21 from a connection condition to a cutting condition to suitable timing based on the event generated in WAN3.

[0030] Moreover, a change in the connection condition of the circuit switch section 21 and cutting condition by the control section 22 can also be carried out by the time amount which a timer clocks. For example, neither synchronous application, mail, delivery of news, transfer of a file nor backup can be performed if it does not necessarily connect always. Then, what is necessary is to make the circuit switch section 21 into a connection condition in the time zone set beforehand according to the time amount which a timer clocks, and just to deliver and receive such data. In addition, although a timer is in the outside of a control section 22 also as that with which control-section 22 the very thing is equipped and enabled the input of a hour entry at the control section 22, it may be any.

[0031] With the gestalt of the above-mentioned operation, LAN1 and WAN3 should be connected through the circuit switch section 21. On the other hand, it is possible to also constitute the network connection system of a configuration of to have used the fire wall together to connection between LAN1 and WAN3.

[0032] Drawing 2 is the block diagram which used the fire wall together and in which showing the network connection structure of a system of other configurations. In this network connection system, the fire wall 23 is further

formed between the circuit switch section 21 and LAN1. But the location of a fire wall 23 may be between the circuit switch section 21 and WAN3.

[0033] Suppose that the computer 11 in LAN1 had unlawful access from WAN3 in the network system of drawing 2 . Here, if the circuit switch section 21 is in the connection condition, the unlawful access will reach even a fire wall 23. Next, although a fire wall 23 filters access from WAN3, since it is unlawful access, it is not told to the computer 11 in LAN1. By such configuration, prevention of unlawful access is strengthened and a system with still higher security can be built rather than the system to the computer 11 in LAN1 from WAN3 shown with the gestalt of the above-mentioned operation.

[0034] Drawing 3 is the block diagram which used the fire wall together and in which showing the network connection structure of a system of other configurations further. In this network connection system, LAN1 and WAN3 are connected through the fire wall 2, and the circuit switch section 21 and a control section 22 are realized as a function of a fire wall 2. The fire wall 2 contains the alarm generating section 24 which emits an alarm, when the computer 11 in LAN1 has unlawful access from WAN3.

[0035] Here, when the alarm generating section 24 generates an alarm, a control section 22 sends a control signal to the circuit switch section 21 so that LAN1 and WAN3 may be in a cutting condition. When there is access to WAN3 from

the computer 11 in LAN1 after the circuit switch section 21 was changed to the cutting condition for example, a control section 22 can send a control signal to the circuit switch section 21 so that it may be in a connection condition again. In addition, a control section 22 can be controlled to change the circuit switch section 21 to a cutting condition, also when various events which were described above occur besides when the alarm generating section 24 generates an alarm.

[0036] Since it not only does not tell the unlawful access as a fire wall 2, but the circuit switch section 21 is made into a cutting condition when there is unjust access from WAN3 to the computer 11 in LAN1, prevention of unlawful access can be strengthened more with having considered as such a configuration. Thereby, a system with still higher security can be built rather than the system shown with the gestalt of the above-mentioned operation.

[0037] With the gestalt of the above-mentioned operation, LAN1 was made into the internal network and the network connection system by which WAN3 as an external network was connected to this was explained as an example. However, the circuit switch section 21 and the control section 22 which described LAN and LAN above or more in any one of LANs of it even in the network system connected with the router etc., for example can be prepared.

[0038]

[Effect of the Invention] As explained above, while being able to prevent unjust

access from an external network to each computer connected to the internal network according to this invention, the data in an internal network can be exchanged convenient.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the network connection structure of a system concerning the gestalt of operation of this invention.

[Drawing 2] It is the block diagram showing the network connection structure of a system concerning the gestalt of other operations of this invention.

[Drawing 3] It is the block diagram showing the network connection structure of a

system concerning the gestalt of other operations of this invention.

[Drawing 4] It is the block diagram showing the network interface module with a security switch concerning the conventional example.

[Description of Notations]

1 LAN

2 Fire Wall

3 WAN

11 Computer

21 Circuit Switch Section

22 Control Section

23 Fire Wall

24 Alarm Generating Section